

د. عدمان مريزق
المدرسة العليا للتجارة

بوقلاشي عماد
المدرسة العليا للتجارة

مداخلة بعنوان:

الأمن المعلوماتي في ظل التجارة الالكترونية

- إشارة إلى حالتي تونس والجزائر-

الملخص

الإنترنت ليست ناضجة بعد من الناحية الأمنية، الأمر الذي يفرض على المنظمات القيام بالمراقبة على جميع أنظمتها ومختلف تطبيقاتها في التجارة الإلكترونية؛ كما يجب عليها أن تكون سباقة ومرنة في مجال الأمن المعلوماتي. فالمؤسسات التي تنجح في حماية أنظمتها وتحسن التكيف مع رهانات التجارة الالكترونية ستملك ميزة تنافسية مقارنة بمنافسيها.

يهدف هذا البحث إلى عرض الجهود الدولية في مجال تفعيل الأمن المعلوماتي ومضمون التجربة التونسية، بالإضافة إلى عرض مظاهر أمن المعاملات الإلكترونية في القانون الجزائري.

Résume

L'Internet n'est pas encore arrivé à maturité en matière de sécurité, ce qui demande aux organisations des contrôles importants aux niveaux de leurs systèmes et des différentes applications du commerce électronique. Les organisations doivent donc être pro-actives et flexibles dans le domaine de la sécurité informatique . Les entreprises qui réussiront à sécuriser leurs systèmes et qui sauront s'adapter aux défis du commerce électronique auront demain un avantage comparatif sur leurs concurrents.

La pressente recherche viser a exposer les progrès internationaux en matière de sécurité informatique et l'expérience tunisienne dans ce domaine, et enfin le cadre réglementaire des transactions électroniques en Algérie.

mots clés : Internet, commerce électronique , sécurité.

المقدمة

يعد الأمن أبرز العناصر اللازمة لتوفير بيئة مناسبة لبناء مجتمع المعلومات في ظل توسع نطاق الإنترنت،حيث أصبح المجرمون المعلوماتيون المحترفون قادرين على إيجاد فرص جديدة في البيئة الرقمية القابلة للخرق، وذلك للقيام بأعمال إجرامية ضدها أو ضد البنى الأساسية الوطنية الحرجة، كشبكات الاتصالات وشبكات النقل والشبكات الخاصة بالمعلومات الصحية .وأصبحت البرمجيات الخبيثة والاعتداءات على الشبكات والنظم عن بعد معروفة بالنسبة إلى مستخدمي شبكة الإنترنت، ولا ينجو منها إلا المستخدمون المحصنون .ويضاف إلى هذه المخاطر الانتشار الواسع للبريد الدعائي، وكذلك الإعلانات الخادعة التي تجتاح البريد الإلكتروني وغيرها.

وبناء على ما سبق، تتمحور إشكالية البحث في السؤال الجوهري التالي:

كيف يسهم الأمن المعلوماتي في ترقية التجارة الإلكترونية ؟

ويتفرع عن السؤال أعلاه جملة من الأسئلة، تتمثل فيما يلي:

- ماهي عناصر الأمن المعلوماتي ؟
- ما هي الجهود الدولية في مجال تفعيل الأمن المعلوماتي ؟
- ما هو مضمون التجربة التونسية في مجال الأمن المعلوماتي؟
- ما هي مظاهر أمن المعاملات الإلكترونية في القانون المدني الجزائري ؟

أولا: عناصر الأمن المعلوماتي والجهود الدولية لضمانه

نرى من المفيد قبل التطرق لعناصر الأمن المعلوماتي والجهود الدولية لضمانه، أن نتناول مفهومه ومراحل تطوره، على النحو التالي:

1- ماهية الأمن المعلوماتي

الأمن المعلوماتي أو أمن المعلومات، من زاوية أكاديمية، "هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاوية قانونية، فان أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة"، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها(**1**).

2- مراحل تطور مفهوم الأمن المعلوماتي

يمكن عرض تطور مفهوم الأمن المعلوماتي فيما يلي(**2**):

منذ أن وجدت المعلومة كان الحفاظ عليها يعتبر غاية في حد ذاته، والجديد في الأمر هو انتقال المعلومة من الشكل اليدوي في الحصول عليها وخزنها واستعمالها ونشرها، إلى استخدام تكنولوجيا المعلومات في إجراء كل ذلك، فمفهوم الأمن المعلوماتي مر بمراحل عدة أدت إلى ظهور ما يسمى بأمنية المعلومات، والمفهوم الجديد لأمنية المعلومات يدور حول تحديد عملية الوصول غير المرغوب به للمعلومات وفق أنظمة

متزامنة مع التطورات المتعاقبة والسريعة في العالم. وفيما يلي بيان لأهم التطورات التي عرفها أمن المعلومات:

 خلال فترة الستينات من القرن الماضي كان مفهوم الأمنية يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة، وكان أول ظهور لمصطلح أمن الحواسيب والذي يعني حماية الحواسيب وقواعد البيانات، ونتيجة للتوسع في استخدام أجهزة الحاسوب تغير الاهتمام ليمثل السيطرة على البيانات وحمايتها.

ورافق ذلك استخدام كلمات البيانات Data Security وشهدت فترة السبعينات الانتقال إلى مفهوم أمن سر بسيطة للسيطرة على الوصول للبيانات، إضافة إلى إجراءات لحماية مواقع الحواسيب من الكوارث، واعتماد خطط استرجاع سريعة للبيانات، وخزن نسخ إضافية لها وللبرمجيات بعيدا عن موقع الحاسوب.

 أما في مرحلة الثمانينات والتسعينات فقد ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات والاتصالات بالسماح لأكثر من مستخدم بالمشاركة في قواعد البيانات، فقد كانت مرحلة أمن المعلومات، حيث أدى التركيز على المعالجات الدقيقة إلى انتقال الأمنية من البيانات إلى المعلومات من حيث المحافظة على المعلومات وتكاملها وتوفرها ودرجة توثيقها لتقليص اختراقها والتلاعب بها وكانت شركة **IBM** الأمريكية أول من وضع تعريف لأمن المعلومات، وكانت تركز على حماية البيانات من حوادث التزوير، والتدمير أو الدخول غير المشروع على قواعد البيانات، وأشارت الشركة إلى أن الأمن التام للبيانات لا يمكن تحقيقه ولكن يمكن تحقيق مستوى مناسب من الأمنية.

- يرى البعض أن بداية القرن الواحد والعشرين هي مرحلة أمن المعرفة وذلك لانتشار الذكاء الاصطناعي وازدياد معدلات تناقل البيانات والتفاعل بين المنظومات والشبكات وصغر حجم أجهزة الحاسوب المستخدمة والتطورات الأخرى التي ستمركز تطبيقات المعارف البشرية.

3- غياب الأمن المعلوماتي كأحد معوقات التجارة الإلكترونية

على الرغم مما توفره التجارة الإلكترونية من مزايا عديدة، فإن هناك من المعوقات ما يقف في طريق التوسع في الأخذ بها بصورة تجعلها البديل الحديث للتجارة التقليدية ، ومن هذه المعوقات ما يرجع إلى طبيعة هذا النوع من التجارة ذاتها ، ومنها ما يرجع إلى الظروف المحيطة بها وذلك على النحو الذي نوجزه فيما يلي(**3**) **:**

- غلبة عنصر المخاطرة في التجارة الإلكترونية نتيجة لضعف الثقة فى التعامل بهذه الطريقة سواء لجديتها أو لسهولة التلاعب في المعاملات التي تجرى بواسطتها.
- عدم كفاية عناصر الأمان بالنسبة لوسائل السداد.
- صعوبة التعامل فى كثير من الأحيان نتيجة لتعدد المقاييس المعيارية التى تطبقها الدول المختلفة فى هذا الشأن.

• الخشية من اختراق المواقع التجارية من جانب قراصنة الإنترنت وهو ما يحدث الآن بشكل واسع حتى وصل الأمر مؤخراً إلى اختراق موضع شركة مايكروسوفت ذاتها وما ترتب على ذلك من خسائر مادية ضخمة.

• تأثير التجارب السيئة لعمليات النصب من جانب الشركات أو حتى من جانب بعض المستهلكين على الشبكة.

• لقصور فى تطبيق قواعد حماية الملكية الفكرية فى العديد من التشريعات.

• عدم وجود تشريعات متكاملة تنظم التجارة الإلكترونية وما يتعلق بها من موضوعات.

• التعارض بين تشريعات الدول في هذا الشأن مما يتعارض مع طبيعة هذا النوع من التجارة.

4- عناصر أمن المعلومات

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات، سواء من الناحية التقنية أو الأدائية، وكذا هدف التدابير التشريعية في هذا الحقل، ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها(**4**):

- السرية أو الموثوقية (CONFIDENTIALITY): وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

- التكاملية وسلامة المحتوى (INTEGRITY): التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

- استمرارية توفر المعلومات أو الخدمة (AVAILABILITY): التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.

- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به (Non-repudiation): ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار انه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات إن تصرفا ما قد تم من شخص ما في وقت معين.

وتطالب كل من منظمة التعاون والتنمية الاقتصادية والاتحاد الأوربي في العديد من التقارير المتعلقة بالإدارة الإلكترونية ضرورة الالتزام بأربعة وظائف أو مستويات أساسية لضمان تأمين أنظمة المعلومات والإدارة الالكترونية وهي(**5**):

- **الخصوصية**: ويقصد بالخصوصية، أن عملية الولوج إلى المعلومات المتاحة في شكل إلكتروني تقتصر فقط على الأطراف المشاركة في الاتصال (الأشخاص، والتطبيقات، والبرمجيات، والأجهزة)، وتستند الخصوصية على مبدأ التشفير الذي يمكن إجرائه على البيانات والمعلومات.

- **وحدة البيانات واستقامتها**: يؤدي الالتزام بوحدة البيانات واستقامتها إلى ضمان أن المعلومات المتبادلة لم يتم التدخل فيها أو تعديلها وذلك في الفترة ما بين إرسالها من جانب المرسل واستقبالها بواسطة المرسل إليه. وجدير بالذكر أنه بدون الاستناد إلى تطبيقات التوقيع الإلكتروني، من العسير اكتشاف أي تعديلات أو تغييرات تطرأ على مستند أو نص معين. ويجب في بعض الحالات، ضمان هذه الاستقامة طوال الفترة التي يتم فيها الاحتفاظ بالبيانات والمعلومات. كما أن عملية أرشفة مستند معين والتوقيع الخاص به يجب أن يكون مؤمنا بهدف تفادي أي تعديلات يمكن أن تطرأ عليه فيما بعد.

 عدم التنصل (عدم القدرة على الإنكار): المقصود بعدم التنصل أو عدم النكران، أنه لا يمكن لأي طرف من الأطراف المشاركة في عملية التراسل إنكار القيام بالمعاملة أو الإجراء، ولضمان عدم النكران لا بد أن تتوافر إمكانية التتبع المستمر للمعاملة التي يتم القيام بها. وبالتالي معارضة أي رفض لها من خلال الإثبات الحاسم بالقيام بها. ويتعلق هذا الأمر باستخدام مجموعة متنوعة من آليات التوقيع الإلكتروني منها منظومة تأكيد الإرسال والاستقبال والاستناد إلى تقنية تعمل على ضمان الحصول على تاريخ ووقت إجراء المعاملة، وهذه التقنية يطلق عليها العمل على أرشفة المعاملة والتوقيع المرتبط بها.

- **التحقق(التعرف على المستخدم)**: ويكمن الهدف من وراء التحقق أو التوثيق إلى التأكد من أن هوية المستخدم، سواء كانت(اسم مستعار، أو حقيقي، أو عنوان IP...) ، تكون هوية متعارف عليها.

ويتوافر أساليب أساسية يمكن الاستعانة بها من أجل التعرف على المستخدم ومنها:

. التحقق والتوثيق من خلال تقنيات التعرف على اسم المستخدم وكلمة السر خاصته.

. إمكانية التحقق أو التوثيق من خلال امتلاك وسيط مادي يستخدم في عملية التحقق مثل (البطاقات الذكية، وبطاقات USB).

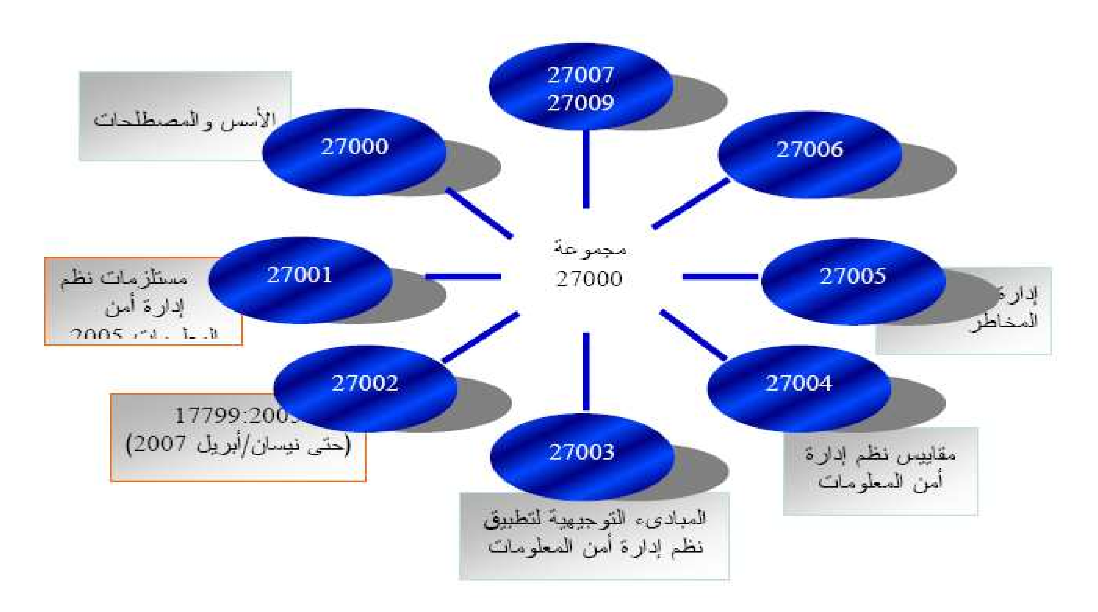
ويؤدي الربط بين الأسلوبين(الوسيط المادي إلى جانب كلمة السر) إلى رفع معدل التأمين، وذلك لأنه يضمن أن مستخدم الوسيط المادي هو صاحبه ومالكه الشرعي. وهو ما يطلق عليه التحقق الفعال أة تحقق ذو عاملين.

ويعتبر التحقق أمر أساسي في استخدام التطبيقات والخدمات المتاحة عن بعد، ويمثل اختيار أسلوب التحقق الذي يسمح بإمكانية الوصول إلى مختلف تطبيقات نظام المعلومات، من المسائل الجوهرية المرتبطة بسياسات التأمين. كما ترتبط عملية الميكنة المستمرة للخدمات (داخل المؤسسة وخارجها) بتقديمها وفقا للسمات الشخصية لمجتمع المستفيدين، وبناء عليه فإن عملية الميكنة تقع في قلب نظام المعلومات المسئول عن إدارة الهويات الإلكترونية والصلاحيات المرتبطة التي تجعل من الأهمية إمكانية التفاعل والعمل المتبادل بين الأنظمة، وفي نفس الوقت التأكيد على سهولة الاستخدام من جانب المستخدم النهائي.

5- الجهود الدولية في مجال الأمن المعلوماتي

قامت المنظمة الدولية لتوحيد المقاييس خلال السنوات الأخيرة بوضع مخطط لسلسلة من المعايير المتعلقة بأمن المعلومات وإدارة المخاطر، وأنشأت مجموعة متكاملة من معايير أمن المعلومات عرفت بمجموعة المعايير المعنية بنظم إدارة أمن المعلومات أو **ISO27k** وهي مبينة في الشكل التالي:

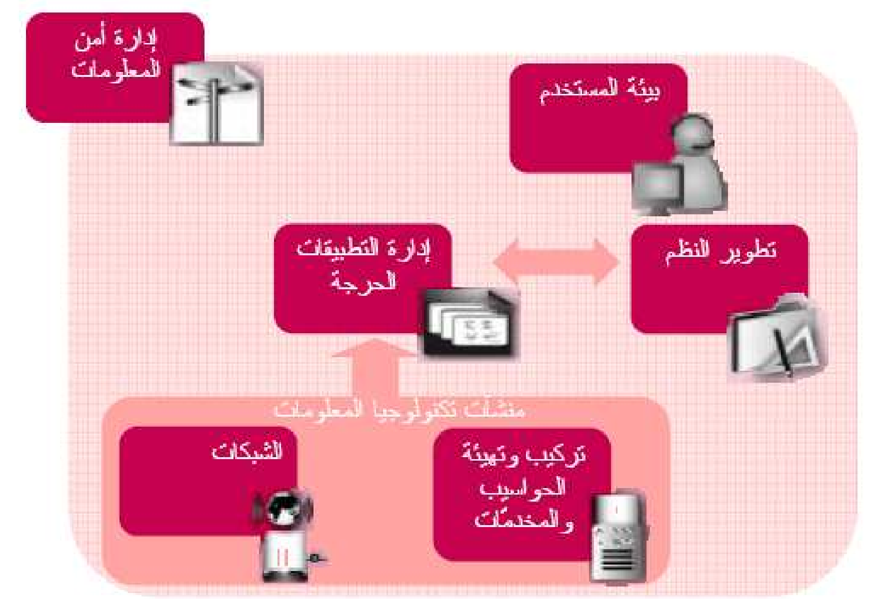
الشكل(1): مجموعة معايير ISO27K



المصدر: اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، بناء بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا، 10 مارس 2009، ص 65.

إضافة إلى المعايير الصادرة عن المنظمة الدولية لتوحيد المقاييس، صدر عن منتدى أمن المعلومات في عام1996 معيار الممارسات السليمة((Standard of Good Practice (SoGP). ويضم هذا المعيار، الذي يتم تحديثه كل عامين، مجموعة من الوثائق التفصيلية للإجراءات الفضلى، والممارسات الواجب إتباعها من أجل حماية المعلومات والنظم الحاسوبية على المستويين المؤسسي والفردي .ويعتمد هذا المعيار على تقسيم إجراءات أمن المعلومات إلى ستة تصنيفات رئيسة مبنية في الشكل التالي:

الشكل (2): التصنيفات الأساسية في معيار الممارسات السليمة



المصدر: اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا، 10 مارس 2009، ص 67.

ثانيا: التجربة التونسية في مجال الأمن المعلوماتي

سوف نتطرق لمحتوى التجربة التونسية في مجال الأمن المعلوماتي و مبادرات التوعية التي تبنتها فيما يلي:

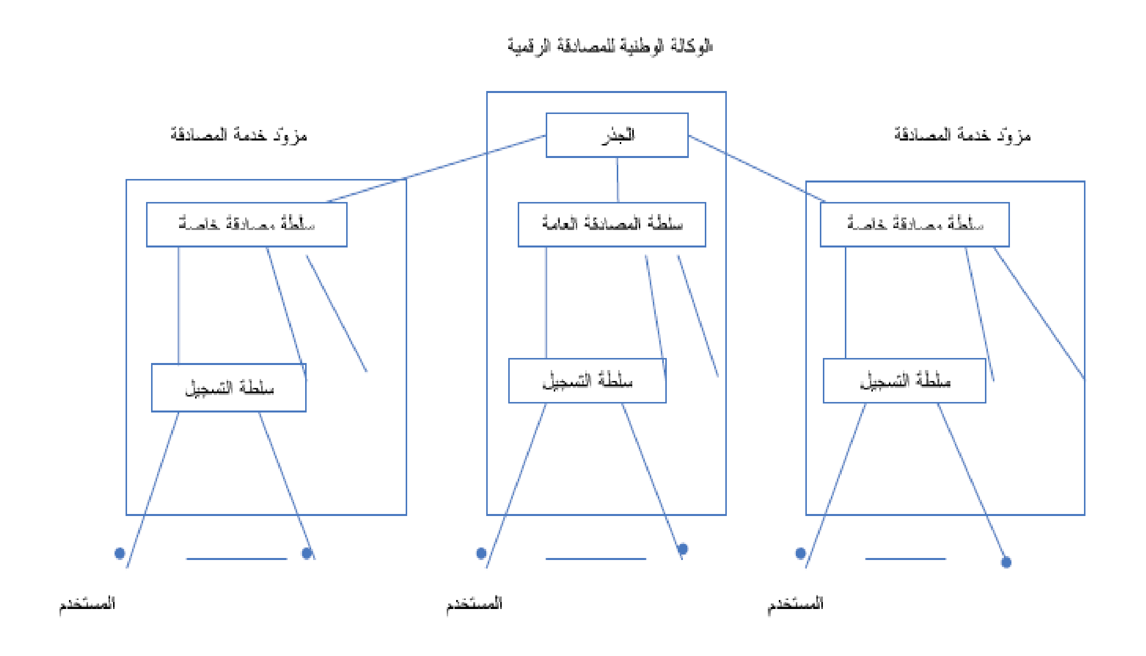
1- **مضمون التجربة**

صدر في تونس مؤخرًا عدد من القوانين والمراسيم التي تحدد التنظيم على المستويين الإداري والمالي، والأدوار المضطلع بها في الوكالة الوطنية لأمن المعلوماتية، والوكالة الوطنية للمصادقة الإلكترونية، إضافة إلى واجبات سلطات التسجيل، ومزودي خدمة المصادقة. وتتناول هذه القوانين والمراسيم موضوع حماية الخصوصية، وشروط استخدام أدوات التشفير وتحديد التعاريف الخاصة بالوثائق الرقمية، وشهادات المصادقة الرقمية، والتوقيع الإلكتروني .وقد أنشئت الوكالة الوطنية للمصادقة الإلكترونية بموجب القانون 2000- 83 المؤرخ 9 آب/أغسطس 2000 والمتعلق بتنظيم المداولات الإلكترونية، والتجارة الإلكترونية وقد كلفت الوكالة بمنح شهادات المصادقة الرقمية أو تجديدها أو إلغائها، والترخيص لمزودي خدمة المصادقة، والتوثق من صحة شهادات المصادقة الأجنبية، وتقييم أجهزة التشفير. وقد وضعت البنية الأساسية للمفاتيح العمومية التي تضم سلطة مصادقة مركزية يتبعها عدد من السلطات الفرعية الموزعة جغرافيا. وتؤدي الوكالة الوطنية للمصادقة الإلكترونية دور السلطة الجذر، وهي تتمتع بأعلى درجات الموثوقية في مجال المصادقة الرقمية، وأمن المداولات الإلكترونية في تونس . وتناط بها الخدمات التالية(6):

• ضمان أمن المداولات الإلكترونية في مجالي التجارة الإلكترونية والحكومة الإلكترونية؛
• إدارة الشهادات الرقمية؛
• منح مزودي خدمة المصادقة الترخيص اللازم؛
• وضع الحلول المتعلقة بالتوقيع الإلكتروني وبضمان أمنه؛
• التأهيل في مجال التوقيع الإلكتروني.

وتعمل الوكالة الوطنية للمصادقة الإلكترونية في تونس على تزويد الجهات الحكومية والعامة بشهادات المصادقة، وهي المسؤولة عن التحقق من الشهادات بالتقاطع مع الهيئات العالمية . ويشير الشكل إلى هيكلية سلطات المصادقة الرقمية في تونس.

الشكل(3):البنية العامة لسلطات المصادقة الرقمية في تونس



المصدر: اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا، 10 مارس 2009، ص 71.

من جهة أخرى، ودائمًا في سياق ضمان أمن المداولات الإلكترونية، تنتشر في تونس عملية التعامل بالنقود الافتراضية، والمقصود بها الدينار الإلكتروني تحديدًا . وهي تعتمد على طبقة المقبس الآمن، وعلى شهادات المصادقة الصادرة عن المكتب المختص .وتتضمن عملية تسديد الفاتورة مرحلة التعرف على بطاقة العميل وتليها مرحلة تخويل هذا العميل تسديد الفاتورة . وقد اعُتمدت هذه الخدمة في البريد التونسي، وأصبحت ُتستخدم لإجراء ما يزيد على 85 في المائة من المداولات الوطنية.

وقد ساعد اعتماد شهادات المصادقة على انتشار عدد من التطبيقات الإلكترونية، كتسجيل الطلاب عن

بعد، واستعمال خدمات الحكومة الإلكترونية، والتصريح عن الضرائب وتسديدها إلكترونيًا . واستطاعت تونس بفضل اعتماد شهادات المصادقة تطوير هذه التطبيقات والخدمات بشكل آمن، وبالتالي نشر خدماتها الإلكترونية عبر شبكة الإنترنت في مجالات عدة كالتجارة الإلكترونية، وتسديد الفواتير إلكترونيًا والحكومة الإلكترونية، والصحة الإلكترونية، والتعليم الإلكتروني، والصيرفة الإلكترونية، وغيرها من العمليات المتطورة .وفي إطار تعزيز أمن المداولات الإلكترونية وثقة المستخدمين بها، تعمل تونس على تنفيذ عدة مشاريع مستقبلية نذكر منها المشاريع التالية:

- تنسيق الإطار القانوني على المستوى الإقليمي؛
- بناء قدرات صانعي القرار والمستخدمين على تغطية المعايير الأمنية؛
- إنشاء مخزن لشهادات المصادقة الجذرية؛
- إنشاء مخزن لجميع شهادات المصادقة المسلمة في البلد؛
- نشر الوعي بالبنية الأساسية، وقضايا الأمن وخدماتها؛
- التركيز على التشغيل البيني من خلال الشراكة مع المنتديات الإقليمية؛

- استخدام تقنيات التشفير لحماية البيانات والوثائق عند نقلها بالبريد الإلكتروني.

2- مبادرات التوعية بأهمية الأمن المعلوماتي في تونس

تعنى الوكالة الوطنية لأمن المعلوماتية في تونس بالتوعية. وهي تتخذ مبادرات عدة لإطلاع كافة شرائح المجتمع على قضايا الأمن والمخاطر، والحلول والمواقف التي يمكن أن تعزز أمن النظم والشبكات .كما تهتم الوكالة بإنشاء منتديات للمناقشة يشارك فيها المهنيون والخبراء، وتساهم في إنشاء

جمعيات تعنى بأمن الحواسيب. وبهدف رفع مستوى الوعي بأمن استخدام تكنولوجيا المعلومات والاتصالات، تقوم الوكالة بنشر عدة برامج للتوعية بأمن نظم المعلومات والشبكات عبر موقعها الإلكتروني وتستهدف من خلالها الأهالي والأطفال بصورة خاصة. فيجد الآباء مثلا بعض النصائح التي يفيد التذكير بها، وبعض الاحتياطات البسيطة التي تساهم في حماية أطفالهم من المخاطر المحتملة على شبكة الإنترنت، وتسمح لهم بالسيطرة على استخدام أولادهم للإنترنت.

ويقدم الموقع أيضًا نصائح حول استخدام التقنيات الخاصة بترشيح البريد الإلكتروني الخاص وحمايته من البريد الدعائي. ويقدم البرمجيات المضادة التي يمكن تحميلها من الموقع مباشرة، كما يعرض دليلا مفصلا حول طريقة استخدام هذه البرمجيات والتحكم بها.

وفي إطار تعزيز أنشطة التوعية، تصدر الوكالة الوطنية لأمن المعلوماتية في تونس مطبوعات متخصصة عديدة في هذا المجال(**7**).

ثالثا: مظاهر أمن المعاملات الإلكترونية في القانون المدني الجزائري

جاء المشرع الإلكتروني بالإثبات الإلكتروني أولا والتوقيع والتوثيق الإلكتروني ثانيا، ويمكن عرض كلاهما فيما يلي:

1- الإثبات الإلكتروني

تنقسم العقود من حيث الإبرام إلى عقود رضائية التي تنعقد بمجرد تبادل رضاء الطرفين المتعاقدين دون الحاجة إلى لصبها في شكل قانوني، كما لدينا طائفة أخرى من العقود تسمى العقود التشكيلية التي تتطلب إفراغها في شكل معين، وهذه الشكلية قد تكون للانعقاد، وبالتالي ركن من أركان العقد عند تخلفها يترتب بطلان العقد، وقد تكون الشكلية فقط للإثبات، ويقصد بالشكلية هي كتابة العقد، وأن هذه الأخيرة قد تكون عرفية وقد تكون رسمية(**8**).

طبقا لنص المادة 333 من القانون المدني الجزائري (**9**) التصرفات القانونية المدنية الغالب فيها هو الكتابة فيما زاد التصرف عن 1000 دج.

والمادة 324 مكرر(10) من القانون المدني الجزائري تنص على " زيادة العقود التي يأمر القانون بإخضاعها إلى شكل رسمي يجب تحت طائلة البطلان، تحرير العقود التي تتضمن نقل ملكية العقار أو حقوق عقارية أو محلات تجارية أو صناعية أو كل عنصر من عناصرها..." .

لكن بصدور القانون 05- 10 المعدل والمتمم للقانون المدني الجزائري(**11**) انتقل المشرع من النظام الورقي في الإثبات إلى النظام الإلكتروني.

حيث أصبح للكتابة في الشكل الإلكتروني مكانا ضمن قواعد الإثبات في القانون المدني الجزائري طبقا لنص المادة 323 مكرر مدني جزائري(**12**) الكتابة في الشكل الإلكتروني ذات التسلسل في أو الأوصاف أو الأرقام أو أية علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة الإلكترونية المستعملة ومهما كانت طرق إرسالها.

ويقصد بالوسيلة الإلكترونية المستعملة مثل القرص الصلب أو القرص المرن أو في شكل رسائل إلكترونية.

وهكذا يتضح مما سبق بأن المشرع الجزائري اعتمد المفهوم الواسع للكتابة المقصود منه سواء الكتابة على الورق أو الكتابة الإلكترونية المثبتة على دعائم غير مادية غير ورقية.

ومن أجل إزالة كل غموض أو نزاع يمكن أن يحدث من الناحية القانونية بشأن تطبيق نص المادة 323 مكرر مدني جزائري، فيما أثار الإشكال " هل للوثيقة الإلكترونية نفس القيمة القانونية في الإثبات مقارنة مع الوثيقة العادية؟"

بموجب المادة 323 مكرر(**13**) جاء المشرع بحل قانوني، ووفقا للقاعدة الفقهية التي تقول لا اجتهاد في وجود النص القانوني، فإن المشرع يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالكتابة على الورق بشرط إمكانية التأكد من هوية الشخص الذي أصدرها.

وبهذا يكون المشرع الجزائري قد سوى بين الكتابة الإلكترونية والكتابة العادية من حيث حجية الإثبات.

غير أن نص المادة 323 مكرر جاء نص مطلق وبالتالي فإن التطبيق المطلق لهذا النص يثير جدال فقهي وقضائي كبير حيث هناك بعض التصرفات ذات أهمية وخطورة من الأفضل أن تبرم في الشكل التقليدي دون الإلكتروني، كرهن الفينة والحقوق الواردة على العقار بصفة عامة وعقد الشركة.

كذلك عدم اتصال بعض التصرفات بالمعاملات الإلكترونية وإنما هي تصرفات شخصية أو مدنية بحتة كالزواج والوصية.

غير أن ما يلاحظ على القانون المدني الجزائري أنه لم يتعرض للنظام القانوني التي تحكم العقد الإلكتروني ولم يتنازل تعريفه، لكن ماهي الوثيقة الإلكترونية؟

إن الوثيقة الإلكترونية أو المحرر الإلكتروني جاءت نتيجة للاستخدام الوسائل الإلكترونية من خلال شبكة الانترنت وإتمام معظم التصرفات القانونية من خلالها.

فنصت المادة الأولى من قانون الأونسترال(**14**) النموذجي بشأن التجارة الإلكترونية على تعريف رسالة البيانات بأنها المعلومات التي يتم إنشائها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية، البريد الإلكتروني، أو البرق أو التلكس أو النسخ البرقي".

2- التوقيع والتوثيق الإلكتروني

لا يكفي اعتراف المشرع الجزائري بالمحرر الإلكتروني كدليل للإثبات، وكما لا يكفي الاعتراف للمحرر الإلكتروني بنفس الحجية التي يتمتع بها المحرر الورقي، لكن يحب أن تتوفر شروط في المحرر الإلكتروني حتى يعتمد عليه في إثبات التصرفات القانونية.

2- 1- التوقيع الإلكتروني:

إعتمد المشرع الجزائري بالتوقيع الإلكتروني لأول مرة في نص المادة 2/327 مدني جزائري المعدلة بالقانون 05- 10(15) والتي تنص على " ... يعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر أعلاه.." وذلك من أجل إضفاء الحجية على المحررات الإلكترونية.

أما عن تعريف التوقيع الإلكتروني، فإن القانون الجزائري يميز بين التوقيع الإلكتروني المؤمن وذلك بموجب المادة 3 من المرسوم التنفيذي 07- 162(16) " التوقيع الإلكتروني هو أسلوب عمل يستجيب للشروط المحددة في المادتين 323 مكرر و323 مكرر (**17**).

التوقيع الإلكتروني المؤمن: هو توقيع إلكتروني يفي بالمتطلبات الآتية:

- يكون خاصا بالموقع.
- يتم بوسائل يمكن أن يحتفظ بها الموقع تحت مراقبته الحضرية.
- يضمن مع الفعل المرتبط به صلة ببحث يكون كل تعديل لاحق للفعل قابلا للكشف عنه.

2- 2- التوثيق الإلكتروني (التصديق الإلكتروني)

الموثق الإلكتروني هو طرف ثالث محايد يتمثل في أفراد أو شركات أو جهات مستقلة محايدة تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية.

والوظيفة الأساسية للموثق الإلكتروني أو لجهة التوثيق الإلكترونية هي تحديد هوية المتعاملين في التعاملات الإلكترونية وتحديد أهليتهم القانونية في التعامل والتحقق من مضمون هذا التعامل وسلامته وكذلك جديته وبعده عن الغش والاحتيال.

ويأخذ التوجيه الأوربي رقم 93 سنة 1999 بفكرة الموثق الإلكتروني وأطلق عليه تسمية مقدم خدمات التصديق وهي نفس التسمية التي جاء بها المشرع الجزائري في المرسوم التنفيذي 07- 162.

وتتطلب ممارسة نشاط التصديق الإلكتروني الحصول على ترخيص تمنحه سلطة البريد والمواصلات السلكية واللاسلكية، وهذا الترخيص يكون مرفق بدفتر الشروط يحدد حقوق وواجبات مؤدي الخدمات والمستعمل(**18**).

أما عن الأشخاص الذين يجوز لهم قانونا ممارسة هذا النشاط، يجب أن تتوفر فيهم نفس الشروط لممارس نشاط تقديم الانترنت في الجزائر(**19**).

إن نشاط مقدمي خدمات التصديق الإلكتروني نشاطا اقتصاديا يخضع للقيد التجاري طبقا للقانون التجاري. وبذلك تكون جهة التوثيق الالكتروني مسؤولة عن توثيق العقد الإلكتروني، الأمر الذي يجعل الوضع تطبيقا لمهمة الموثق العادي.

الخاتمة

لا يقتصر تطوير التجارة الإلكترونية وتكنولوجيا المعلومات في أي بلد على إصدار قوانين متعلقة بالتجارة الإلكترونية وحسب، بل يجب العمل على تطوير رزمة من المجالات. ويجب أن تدرك الدولة والمواطن ورجل الأعمال أهمية الإنترنت والتجارة الإلكترونية في القيام بالأعمال وتوفير الوقت والجهد.

تعتبر المعلومات عنصرًا أساسيًا في حياة الأفراد والمنظمات، ورأس مال لا غنى عنه بالنسبة إلى المؤسسات التجارية في عالمنا اليوم القائم على تكنولوجيا المعلومات والاتصالات . فنظم تكنولوجيا المعلومات تؤدي دورًا رئيسًا في ربط الشبكات الداخلية داخل المؤسسات والمنظمات، أو عبر تأمين الاتصال مع عدد كبير من الموردين والشركاء والعملاء والأسواق. وتساهم هذه النظم، في حال كانت المعلومات المتوفرة بشأنها كاملة ودقيقة ومحدثة، في تحسين عملية اتخاذ القرارات الإدارية . وأما ضمان تقديم معلومات بهذه الجودة الرفيعة، فلا يمكن أن يتم إلا عن طريق الحد من هامش الخطأ . ومن هنا تظهر الحاجة إلى ضمان أمن نظم المعلومات عبر التصدي للأخطار التي تهدد سرية المعلومات وتوفرها وتكاملها.

ولا يكفي وضع سياسة تضمن أمن المعلومات، أو الاستثمار في عدد من المعدات أو التكنولوجيات للحد من المخاطر التي تتعرض لها الشبكة الإلكترونية، أو نظم المعلومات، وإنما يجب إدخال ثقافة أمن المعلومات في صلب السلوك اليومي للأفراد والعاملين كي تصبح جزءًا لا يتجزأ من ثقافة الشركات.

وفي هذا الصدد يمكن تقديم **التوصيات** التالية:

- التدريب الفعال في مجال أمن المعلومات؛
- العمل على استحداث وبصورة مستمرة أساليب جديدة لصد المعتدين ومحترفي الجريمة الإلكترونية؛
- الاستفادة من خبرات المنظمات العالمية في مجال الأمن المعلوماتي؛
- تفعيل دور التعاون الدولي، ولما لا العربي كمرحلة أولى، في مجال محاربة الجريمة الإلكترونية؛
- نشر ثقافة الأمن المعلوماتي بكل السبل الممكنة، كخط دفاع أول الجريمة الإلكترونية.

التهميش

1. يونس عرب، أمن المعلومات، دار المسيرة للطباعة والنشر، الأردن، ص 1- 3.
2. زيدان محمد، محمد حمو، متطلبات أمن المعلومات المصرفية في بيئة الأنترنت، المؤتمر السادس لجمعية المكتبات والمعلومات السعودية، البيئة المعلومات الآمنة: المفاهيم والتشريعات والتطبيقات، المنعقد بمدينة الرياض، خلال الفترة 21- 22 ربيع ثاني 1431 هـ الموافق لـ 6- 7 أبريل 2010.
3. هشام نبيه المهدي محمد، التجارة الإلكترونية (الصور المفهوم والأنماط)، مؤتمر وورشة عمل حول التجارة الإلكترونية وأمن المعلومات .. الفرص والتحديات، القاهرة، الفترة من 16- 20 نوفمبر 2008.
4. يونس عرب، مرجع سابق، ص 3.
5. أحمد فرج أحمد، نحو إطار عام لتطبيق استخدام منظومة التوقيع الإلكتروني في مؤسسات المعلومات دراسة للإطار التقني والتنظيمي و البنية التحتية، دراسات المعلومات، العدد الأول، يناير 2008، ص ص 55- 56.
6. اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، بناء الثقة بالخدمات الإلكترونية في منطقة الإسكوا، 10 مارس 2009، ص 70- 72.
7. اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، مرجع سابق،
8. المادة 324 القانون 88- 14 لـ 3 ماي 1988 المعدل والمتمم للأمر 75- 58 لـ 26 سبتمبر 1975 المتضمن القانون المدني الجزائري.
9. الأمر 75- 58 لـ 26 سبتمر 1975 المتضمن القانون المدني الجزائري المعدل والمتمم.
10. القانون رقم 88- 14 السابق الذكر
11. الأمر 75- 58 السابق الذكر.
12. القانون 05- 10 المعدل والمتمم للأمر 75- 58 المتضمن القانون المدني المعدل والمتمم.
13. نفس القانون المذكور سابقا.
14. لمزيد من التفصيل فيما يخص الأنسترال راجع: معهد أبحاث السياسات الاقتصادية الفلسطيني(ماس)، مراجعة نقدية لمشروعي قانوني المبادلات والتجارة الإلكترونية وتنظيم التوقعات الإلكترونية، 2006.
15. القانون 05- 10 المعدل والمتمم للامر 75- 58 المتضمن القانون المدني
16. المرسوم 07- 162 يعدل ويتمم المرسوم 01- 123 المتعلق بنظام الاستغلال المطبق على كل نوع من أنواع الشبكات بما فيها اللاسلكية الكهربائية وعلى مختلف خدمات المواصلات السلكية واللاسلكية.
17. المادة 323 مكرر و323 مكرر 1 تعرف الكتابة الإلكترونية.
18. ناجي الزهراء ، المؤتمر العلمي المغاربي الأول حول المعلوماتية والقانون، المنعقد في الفترة من 28 إلى 29 أكتوبر 2009، أكادمية الدراسات العليا " طرابلس".
19. المادة 3 من المرسوم 07- 162.